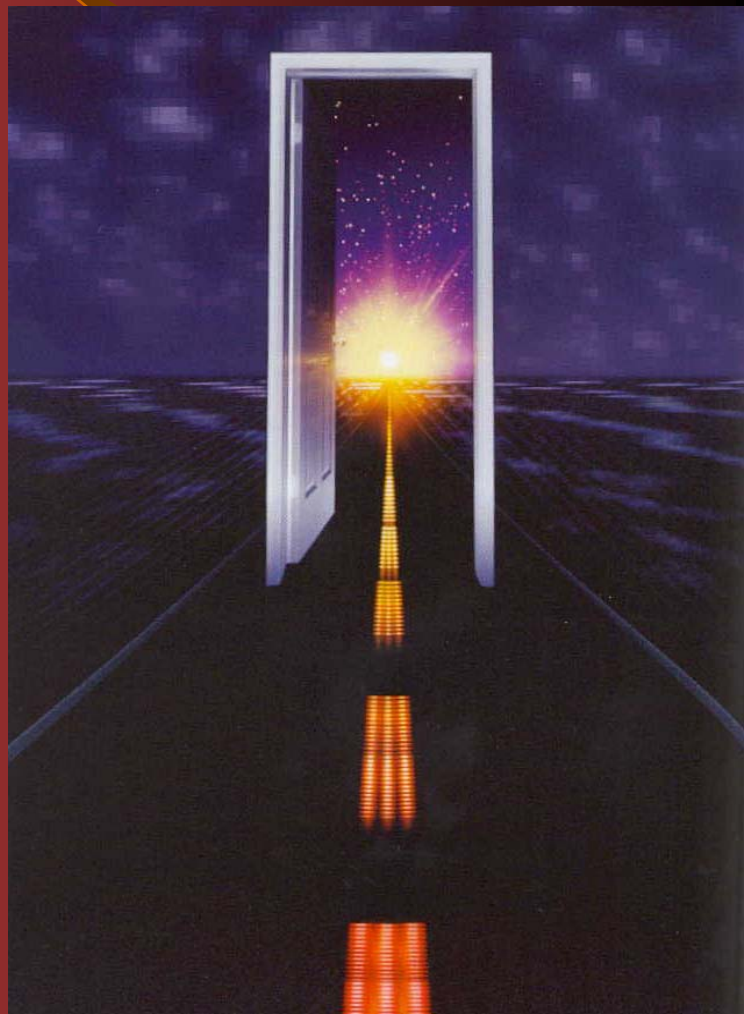
MHCC | MARYLAND HEALTH CARE COMMISSION

HIPAA
A Brief Look Inside

HIPAA
Expected To Evolve Over Time…

- The Secretary (HHS) many adopt a modification to a standard once a year
- The Secretary may adopt a modification at any time during the first year after the standard is adopted
  - Compliance date can be as early as 180 days after modification is adopted
  - Small health plan compliance date can be extended

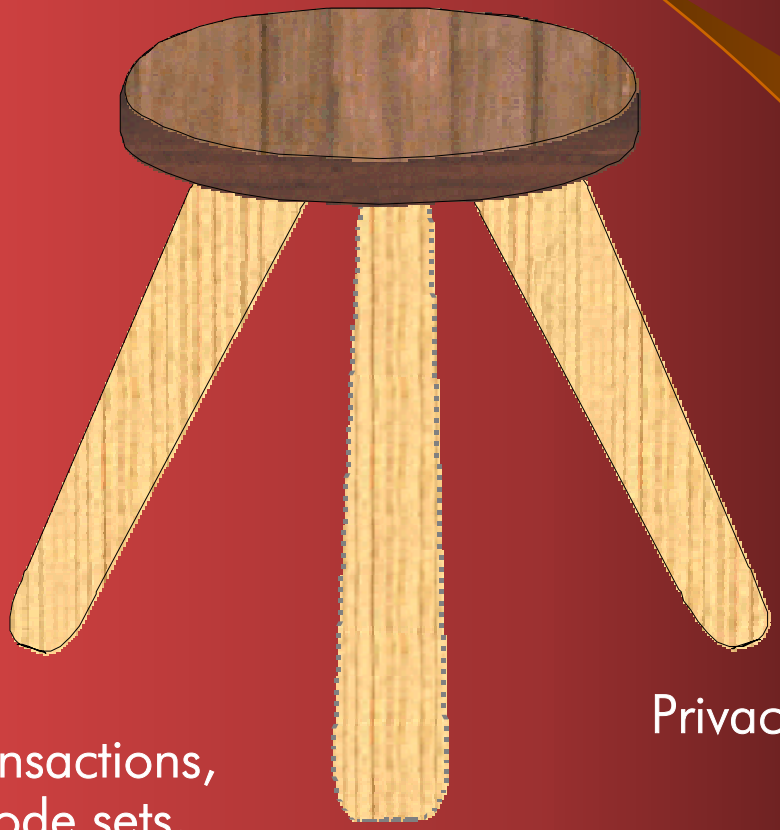


Does HIPAA Apply To Me?

Dentists that exchange protected health care information with another covered entity must comply with HIPAA

- Those excluded from HIPAA today are likely to be effected later on…
  - H.R. 3323
  - Kennedy's proposed Efficiency in Health Care Act, S. 2638
  - Private payer requirements

Administrative Simplification
Three Components



HIPAA
Sound Documentation Is Essential

- Transaction Standards & Code Sets
- Privacy
- Security

HIPAA Enforcement "A Carrot And Not A Stick"

- *Robin Frohboese, Principal Deputy & Acting Director of the Office for Civil Rights* has stated that identified violations are viewed as an opportunity to educate covered entities back into compliance.
  - *"It's critically important that covered entities understand their responsibilities and that we help them with compliance so our enforcement is minimized. If we find violations, we will seek voluntary compliance. It will only be in the most egregious situations where we are not able to get voluntary compliance that we will do other things, such as civil monetary penalties or, in the worst situations, refer to the Justice Department."*

Source: *Report on Patient Privacy*, May 2002

Accountability

- *Civil penalties* against a covered entity that fails to comply
  - $100 per incident
  - Up to $25,000 per person/year/standard violated
  - Enforcement by HHS Office for Civil Rights
- *Federal criminal* penalties for knowingly and improperly disclosing or obtaining protected health information
  - Up to $250,000 and up to 10 years in prison
  - Enforcement by Department of Justice

Compliance Monitoring

- Centers for Medicare and Medicaid Services (CMS) monitors compliance on the transaction and code set standards
- The Office for Civil Rights will monitor compliance on the privacy and security regulations
- Audits can be unannounced
- Keep compliance activities in perspective

HIPAA Transactions Standardize Health Information

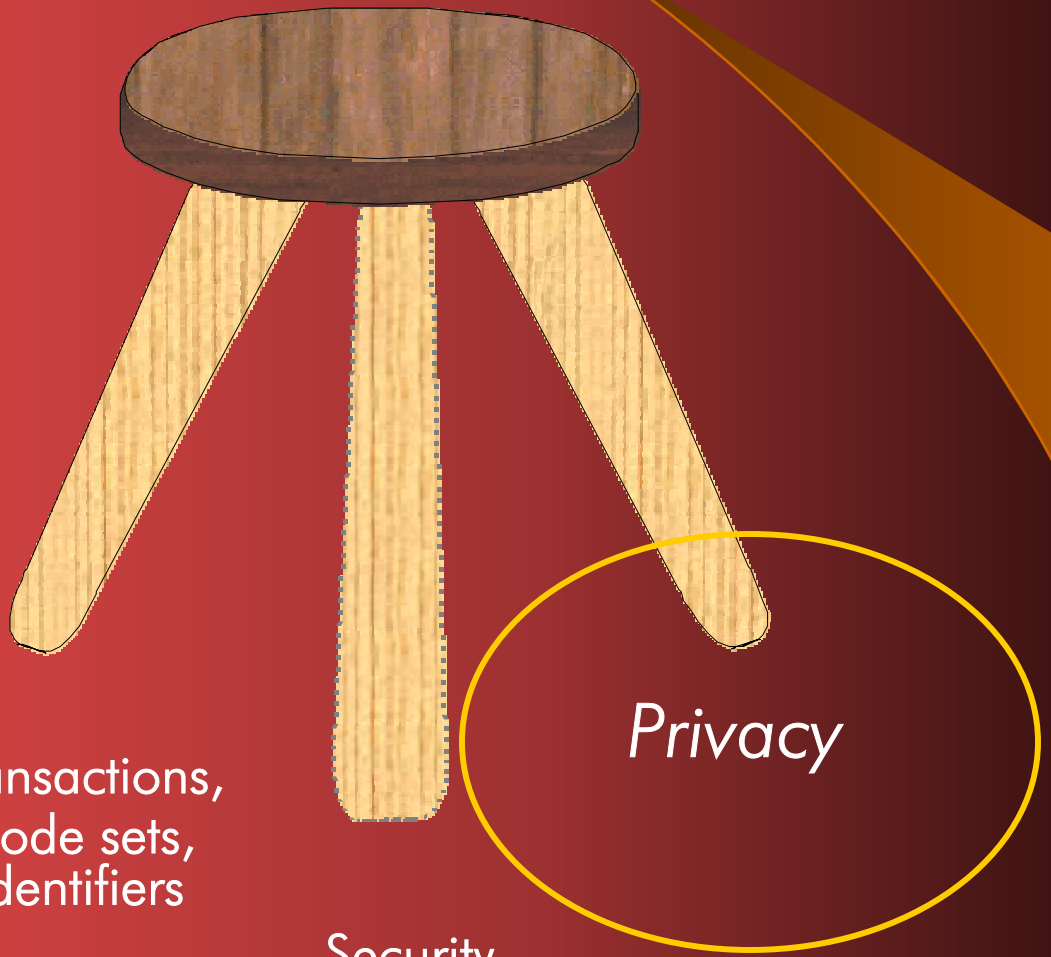
- Payers and electronic health networks must be capable of electronically accepting:
  - Enrollment in a health plan,
  - Eligibility for a health plan,
  - Health claims (retail drug, dental, professional, and institutional)
  - Health care payment & remittance advise
  - Health plan premium payments,
  - Health claim status,
  - Referral certification, authorization, coordination of benefits (Rx: NCPDP Telecommunication Guide)

Transaction Testing Certification Vendors

- Claredi – www.claredi.com
- EDIFECS – www.edifecs.com
- Foresight Corporation – www.foresight.com
- GFEGUSA – www.gfeg.com
- AppLabs, Inc. – www.app;abs.com

HIPAA Transactions…
You Manage The Process

HIPAA
Privacy



Protected Health Information (PHI)
The 19 Identifiers

- Name
- Address
- E-mail
- Dates
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate Number
- License Number
- Vehicle Identifiers
- Facial Photographs
- Telephone Numbers
- Device Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Geographic Units
- Any Other Unique Identifier Or Codes

Consent - Optional

- A consent allows a provider to use or disclose protected health care information to carry out treatment, payment, & health care operations
- One time only:
  - Inform that protected health information may be used or disclosed for treatment, payment, or health care operations
  - Refer to notice of privacy practices
  - State the right to request restrictions
- May condition treatment based on consent
- May be revoked
- Provider must document & retain consent forms
- Attempts to obtain a consent must be documented

Authorization

- Authorization is more detailed and specific than consent
  - Limited to only information to be disclosed
  - Recipient of information
  - Includes an expiration date
- Core elements of a valid authorization
  - A description of the information to be used or disclosed
  - The name or other specific identification of the person authorized to make the requested uses and disclosures
  - An expiration date or expiration event
  - A statement of the individuals right to revoke the authorization in writing
  - A statement that information used or disclosed may be subject to re-disclosure by the recipient
  - Signature of the individual and date
- Authorizations must be written in plain language

Notice Of Privacy Practices - Elements

- Notice can be layered with summary information at the top and more detailed information at the bottom
  - *Header:* This notice described how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. Clarification of an individuals privacy rights
  - *A description and at least one example* of the types of uses and disclosures
  - *A description of each of the purposes* for which the covered entity is permitted or required to disclose PHI

Notice Of Privacy Practices - Elements
(Continued)

- *A statement that uses and disclosures* follow more stringent State or Federal laws
- *A statement that other uses and disclosures* will be made only with the individuals written authorization and that the individual may revoke such authorization
- *Separate statements for certain* uses or disclosures
- *Complaint contact*
- *Contact name* for obtaining other information
- *Effective date*

Notice Of Privacy Practices - Elements
(Continued)

- *Revision practice* and distribution process
- *Providers must provide* on the first date of service
- *Notice must be available on site* for distribution and prominently posted
- *A notice must be maintained on a covered entity's Web site* that provides customer service or benefit information

A Word On Storing Patient Information

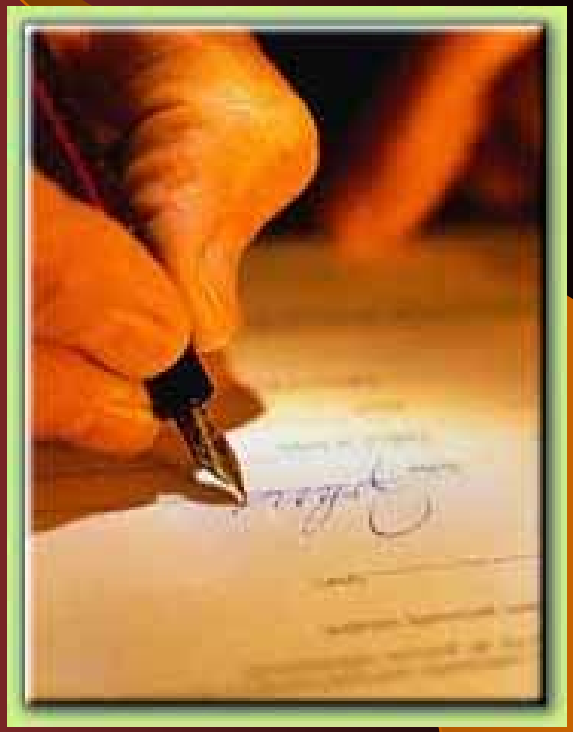
The regulations do not describe the particular measures a covered entity must take to meet the standard, variation is likely to exist among practitioners. Patient files need to be secure within a secure location. Practitioners are not required to guarantee the protection of PHI against all forms of assault. Practitioners are required to develop reasonable policies against theft of PHI.

What About Sign In Sheets?

- HIPAA does not require practitioners to use sign in sheets
- Consider its purpose and value
- Look for opportunities to limit potential disclosure of PHI
- *Evaluate low cost alternatives*

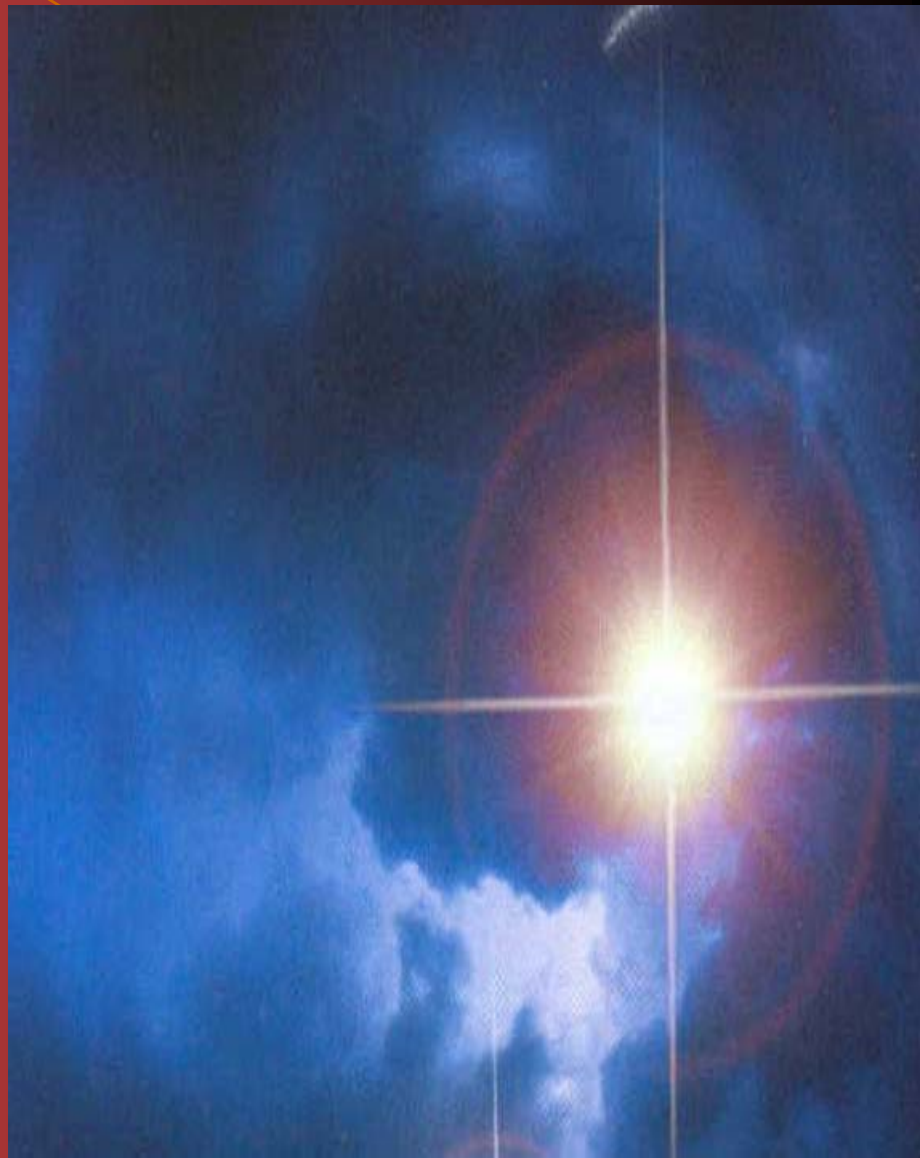
Business Associate Contract
An Agreement Between Parties

- Acts on behalf of a covered entity in conducting activities involving use of PHI
- Covered entities are not responsible for actions of business associates
- Monitoring is not required
- An organization can be both a covered entity and a business associate
- Due April 04



Business Associate Contract
(Continued)

- Limit contents to information specific to PHI
- Trading partners will be reluctant to sign complex Business Associate Contracts
- Trading partners are less likely to incur legal fees on easy to read Business Associate Contracts
- Keep it simple



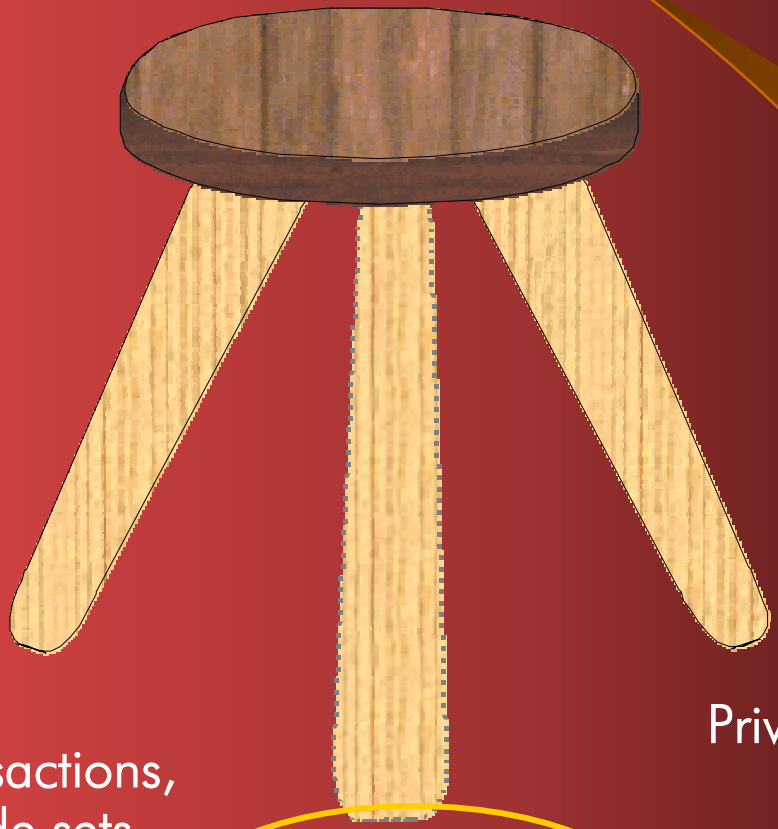
Administrative Requirements

- Implementation allows for flexibility and scalability
  - Response can be geared to your environment
- Covered entities are required to:
  - Designate a privacy official
  - Develop policies and procedures
  - Notices of practices
  - Provide privacy training to its workforce
  - Develop a system of sanctions for employees who violate the entity's policies
  - Meet documentation requirements

Administrative Requirements (Continued)

- A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law
- When a covered entity changes a privacy practice that is stated in the notice, it may make the change effective for PHI that was created or received prior to the date of the notice providing the notice reserves the right to make such change in its privacy practices
- A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented

HIPAA
Security "Proposed"



Transactions,
Code sets,
Identifiers

Privacy

Security

HIPAA Security Standards
An Overview

Four Security Categories:

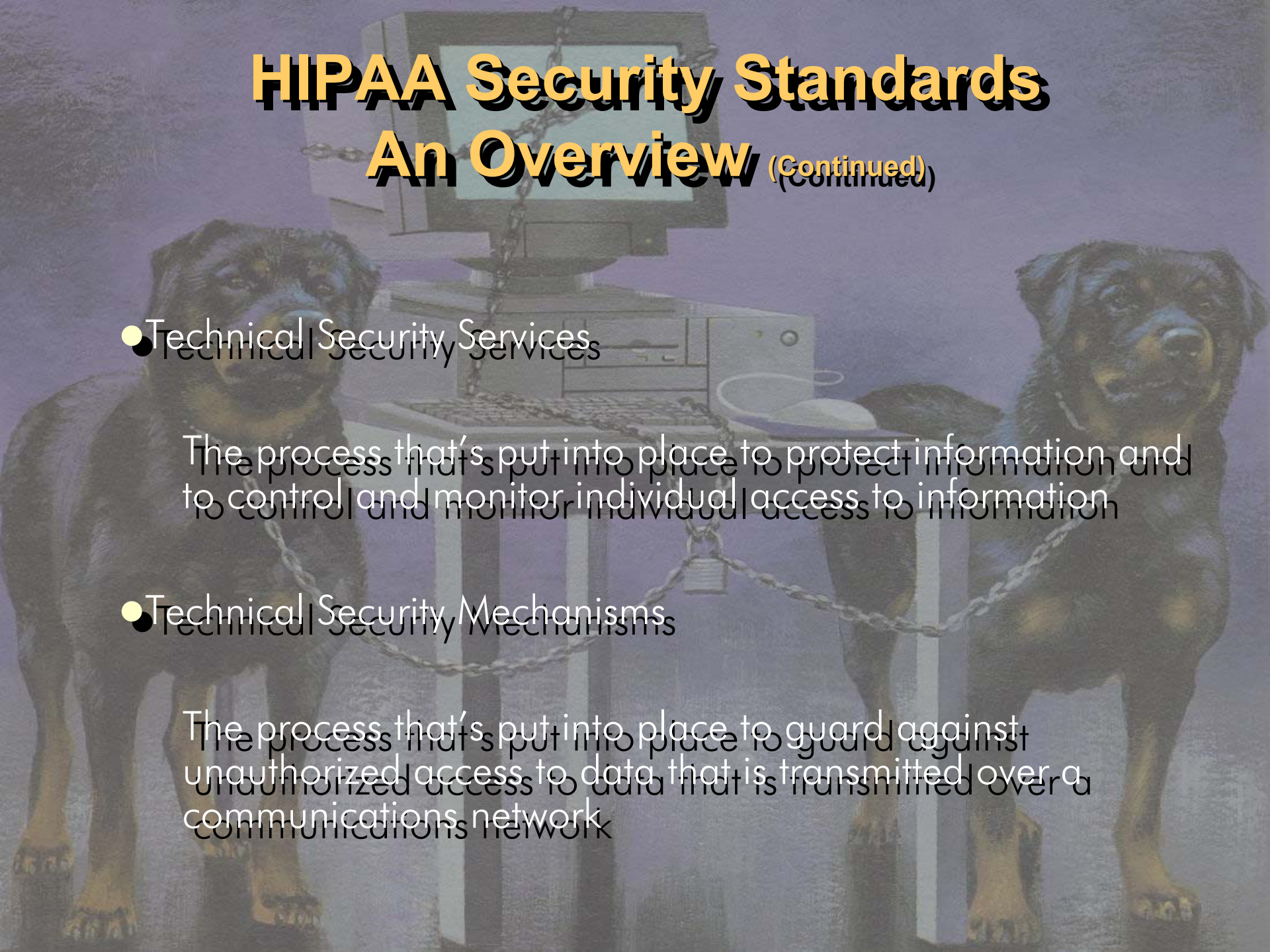
- Administrative Procedures

  Development and implementation of security measures to protect data, and the conduct of personnel in relations to the protection of data

- Physical Safeguards

  The protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as intrusion

HIPAA Security Standards
An Overview (Continued)



- Technical Security Services

  The process that's put into place to protect information and to control and monitor individual access to information

- Technical Security Mechanisms

  The process that's put into place to guard against unauthorized access to data that is transmitted over a communications network

Begin Planning for HIPAA

Learn more about the requirements

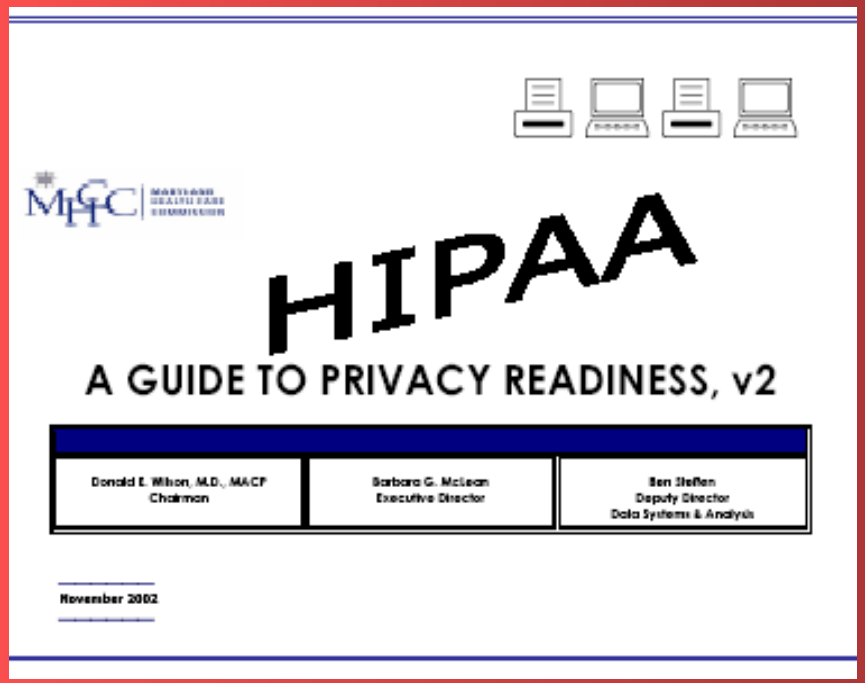
Conduct a gap assessment and develop P&Ps

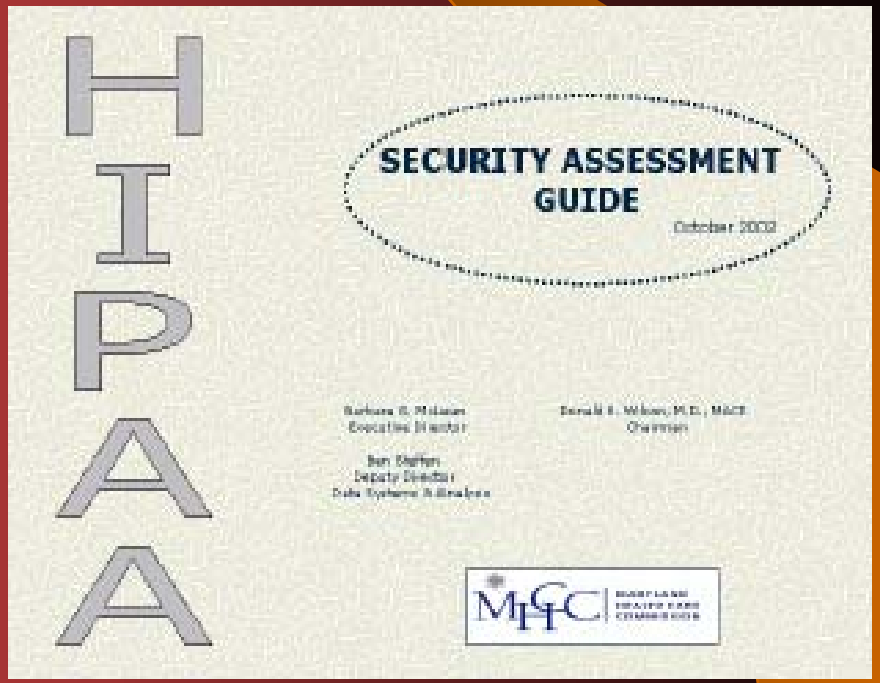
Evaluate current processes against the standards

HIPAA Assistance For Dentists

- An easy to use gap assessment tool for dentists:

  Both are available at the MHCC Web-site





HIPAA– The Change Process

Identify Practitioner Changes

Assessment of Current Knowledge: Skills, Organizational Resources and Change Resistance

Develop and Deliver Policies and Training

Measure and Evaluate Behavioral Changes

Re-evaluate Change Process


Questions?
Maryland Health Care Commission